

Universal Witnesses for State Complexity of Basic Operations Combined with Reversal*

Janusz Brzozowski and David Liu

David R. Cheriton School of Computer Science, University of Waterloo,
Waterloo, ON, Canada N2L 3G1
{brzozo,dyliu}@uwaterloo.ca

Abstract. We study the state complexity of boolean operations, concatenation and star with one or two of the argument languages reversed. We derive tight upper bounds for the symmetric differences and differences of such languages. We prove that the previously discovered bounds for union, intersection, concatenation and star of such languages can all be met by the recently introduced universal witnesses and their variants.

Keywords: basic operation, boolean operation, regular language, reversal, state complexity, universal witness

1 Introduction

For background on state complexity see [2,3,11]. The *state complexity of a regular language* is the number of states in the minimal deterministic finite automaton (DFA) recognizing the language. The *state complexity of an operation* on regular languages is the worst-case state complexity of the result of the operation as a function of the state complexities of the arguments.

The state complexity of basic operations combined with reversal was studied in 2008 by Liu, Martin-Vide, A. Salomaa, and Yu [9]. Let K and L be two regular languages over alphabet Σ , and let their state complexities be m and n , respectively. The basic operations considered in [9] were union ($K \cup L$), intersection ($K \cap L$), product (catenation or concatenation) (KL) and star (L^*), and reversal (L^R) was added to these operations. It was shown that $(2^m - 1)(2^n - 1) + 1$ is a tight upper bound for $(K \cup L)^R = K^R \cup L^R$ and $(K \cap L)^R = K^R \cap L^R$. It was also proved that $3 \cdot 2^{m+n-2} - (2^n - 1)$ is an upper bound for $(KL)^R = L^R K^R$, but the question of tightness was left open. Cui, Gao, Kari and Yu [5] answered this question positively, and also showed that $3 \cdot 2^{m+n-2}$ is an upper bound for $K^R L$. In another paper [6], they proved that $(m - 1)2^n + 2^{n-1} - (m - 1)$ is a tight upper bound for KL^R . Gao, K. Salomaa, and Yu [7] demonstrated that 2^n is a tight upper bound for $(L^*)^R = (L^R)^*$. Gao and Yu [8] found the tight upper bound $m2^n - (m - 1)$ for $K \cup L^R$ and $K \cap L^R$. Thus eight basic operations with reversal added have been considered so far.

* This work was supported by the Natural Sciences and Engineering Research Council of Canada under grant No. OGP0000871.

There are two steps in finding the state complexity of an operation: one has to establish an upper bound for this complexity, and then find languages to act as witnesses to show that the bound is tight. One usually defines a sequence $(L_n \mid n \geq k)$ of languages, where k is some small positive integer. This sequence will be called a *stream* of languages; for example, $(\{a, b\}^* a \{a, b\}^{n-3} \mid n \geq 3)$ is a stream. The languages in a stream normally differ only in the parameter n . Usually, two different streams have been used as witnesses for binary operations.

In 2012, Brzozowski [3] defined the notion of *permutational equivalence*. Two languages K and L over Σ are permutationally equivalent if one can be obtained from the other by permuting the letters of the alphabet. For example, $K = \{a, b\}^* a \{a, b\}^{n-3}$ is permutationally equivalent to $L = \{a, b\}^* b \{a, b\}^{n-3}$. These two languages have the same properties, only the letters have been renamed.

The DFA $\mathcal{U}_n(a, b, c) = (Q, \Sigma, \delta, q_0, F)$ of Fig. 1 and its language, $U_n(a, b, c)$, were proposed in [3] as the “universal witness” DFA and language, for $n \geq 3$. The permutationally equivalent language and DFA of $U_n(a, b, c)$ and $\mathcal{U}_n(a, b, c)$ obtained by interchanging a and b are denoted by $U_n(b, a, c)$ and $\mathcal{U}_n(b, a, c)$. The restriction of the language and the DFA to alphabet $\{a, b\}$ is denoted by $U_n(a, b, \emptyset)$ and $\mathcal{U}_n(a, b, \emptyset)$.

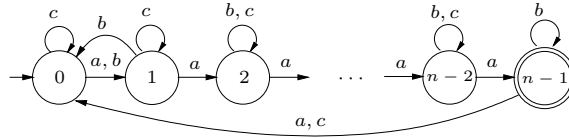


Fig. 1. DFA $\mathcal{U}_n(a, b, c)$ of a complex language $U_n(a, b, c)$.

It was proved in [3] that the bound $2^{n-1} + 2^{n-2}$ for star is met by $U_n(a, b, \emptyset)$, and the bound $(m-1)2^n + 2^{n-1}$ for product, by $U_m(a, b, c)U_n(a, b, c)$. The bound mn for union, intersection, difference $(K \setminus L)$ and symmetric difference $(K \oplus L)$ is met by two permutationally equivalent streams $(U_m(a, b, c) \mid m \geq 3)$ and $(U_n(b, a, c) \mid n \geq 3)$. Thus $U_n(a, b, c)$ is a universal witness for the basic operations.

The inputs to the DFA $\mathcal{U}_n(a, b, c)$ perform the following transformations on the set $Q = \{0, \dots, n-1\}$ of states. Input a is a *cycle* of all n states, and this is denoted by $a : (0, \dots, n-1)$. Input b is a *transposition* of 0 and 1, and does not affect any other states; this is denoted by $b : (0, 1)$. Input c is a *singular* transformation sending state $n-1$ to state 0, and not affecting any other states; it is denoted by $c : \binom{n-1}{0}$. It is known [3] that the inputs of $\mathcal{U}_n(a, b, c)$ of Fig. 1 perform all n^n transformations of states, and also that the state complexity of the reverse of $U_n(a, b, c)$ is 2^n ; the latter result follows by a theorem from [10].

A *dialect* of $U_n(a, b, c)$ is the language of any DFA with three inputs a , b , and c , where a is a cycle as above, b is the transposition of *any* two states (p, q) , and c is a singular transformation $\binom{r}{s}$ sending *any* state r to *any* state $s \neq r$.

The initial state is always 0, but the set of final states is arbitrary, as long as the DFA is minimal.

The universal witness and the notion of dialect have been extended to quaternary alphabets [3], by adding a fourth input d which performs the identity permutation, denoted by $d : \mathbf{1}_Q$. The concepts of permutational equivalence and dialect are extended in the obvious way to quaternary languages and DFA's.

In this paper, we extend the notion of basic operations from [9] by including difference and symmetric difference. Altogether, we study the following 13 languages with these basic operations and reversal:

$$\begin{aligned} & K \cup L^R, \quad K \cap L^R, \quad K \setminus L^R, \quad K \oplus L^R, \quad L^R \setminus K, \\ & K^R \cup L^R, \quad K^R \cap L^R, \quad K^R \setminus L^R, \quad K^R \oplus L^R, \\ & KL^R, \quad K^R L, \quad K^R L^R \text{ and } (K^R)^*. \end{aligned}$$

Our contributions are as follows:

1. We prove the conjecture from [3] that the bound mn for all four boolean operations in the case where $m \neq n$ is met by two identical streams of languages $U_m(a, b, \emptyset)$ and $U_n(a, b, \emptyset)$.
2. We derive the bound $m2^n - (m - 1)$ for $K_m \setminus L_n^R$ and $L_n^R \setminus K_m$ and the bound $m2^n$ for $K_m \oplus L_n^R$, and show that these bounds and the known bounds for $K_m \cup L_n^R$ and $K_m \cap L_n^R$ are met by two identical streams of languages $U_m(a, b, c)$ and $U_n(a, b, c)$. This reduces the size of the alphabet for union and intersection from four in [8] to three.
3. We derive the bound $(2^m - 1)(2^n - 1) + 1$ for $K_m^R \setminus L_n^R$, and the bound 2^{m+n-1} for $K_m^R \oplus L_n^R$, and show that these bounds and the known bounds for $K_m^R \cup L_n^R$ and $K_m^R \cap L_n^R$ are met by two streams, $U_{\{0,2\},m}(a, b, c)$ and $U_{\{1,3\},n}(b, a, c)$, where the set of final states in $\mathcal{U}_{\{0,2\},m}(a, b, c)$ (respectively, $\mathcal{U}_{\{1,3\},n}(b, a, c)$) is $\{0, 2\}$ (respectively $\{1, 3\}$).
4. We prove that the known bound for $K_m L_n^R$ is met by two identical streams of languages $U_m(a, b, c)$ and $U_n(a, b, c)$.
5. We show that the known bound for $K_m^R L_n$ is met by two permutationally equivalent dialects of $U_n(a, b, c, d)$.
6. We prove that the known bound for $(K_m L_n)^R = L_n^R K_m^R$ is met by two permutationally equivalent streams $(U_m(a, b, c, d) \mid m \geq 3)$ and $(U_n(d, c, b, a) \mid n \geq 3)$. Our proof is considerably simpler than the one in [5].
7. We note that the original proof in [7] uses a dialect of $U_n(a, b, c)$, and point out that the known bound is met by $U_n(a, b, c)$ with final state 0.
8. In obtaining the results above, we prove Conjectures 1–4, 8, 11, and 14 of [3].

The remainder of the paper is structured as follows. In Section 2 we deal with boolean operations with no reversed arguments. Boolean operations with one and two reversed arguments are considered in Sections 3 and 4. Product and star and examined in Section 5, and Section 6 concludes the paper.

2 Boolean Operations with No Reversed Arguments

Let $K \circ L$ denote any one of the four boolean operations $K \cup L$, $K \cap L$, $K \oplus L$ and $K \setminus L$. It is well-known that, if m and n are the state complexities of K and L ,

the state complexity of $K \circ L$ is less than or equal to mn . It was shown in [3] that $U_m(a, b, \emptyset)$ and $U_n(b, a, \emptyset)$ are witnesses to this bound, and it was conjectured that $U_m(a, b, \emptyset)$ and $U_n(a, b, \emptyset)$ are also witnesses if $m \neq n$. We now prove this conjecture. The DFA's $\mathcal{D}_1 = \mathcal{U}_4(a, b, \emptyset)$ and $\mathcal{D}_2 = \mathcal{U}_6(a, b, \emptyset)$ are shown in Fig. 2. Their direct product, \mathcal{P} , shown in Fig. 3, serves as a basis for all four cases.

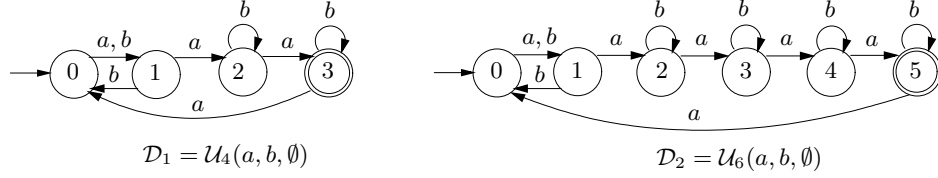


Fig. 2. DFA's \mathcal{D}_1 and \mathcal{D}_2 of $U_4(a, b, \emptyset)$ and $U_6(a, b, \emptyset)$.

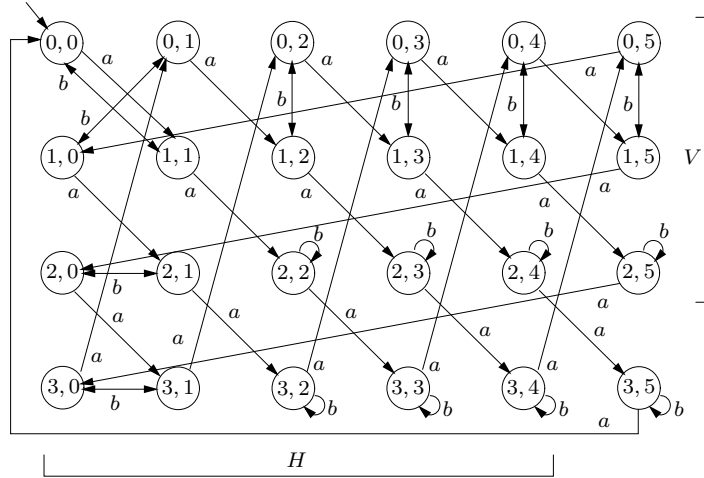


Fig. 3. Direct product \mathcal{P} of $\mathcal{D}_1 = \mathcal{U}_4(a, b, \emptyset)$ with $\mathcal{D}_2 = \mathcal{U}_6(a, b, \emptyset)$.

Theorem 1 ($K_m \circ L_n$, $m \neq n$). *For $m, n \geq 3$ and $m \neq n$, the complexity of $U_m(a, b, \emptyset) \circ U_n(a, b, \emptyset)$ is mn .*

Proof. First it will be shown that all mn states of the direct product are reachable from the initial state $(0, 0)$. Without loss of generality, assume that $m < n$. Throughout the paper, we use the notation $q_1 \xrightarrow{w} q_2$ to say that state q_2 is

reachable from state q_1 by word w . We have $(0, 0) \xrightarrow{a^m} (0, m) \xrightarrow{(ab)^{n-1-m}a} (1, 0)$. For $1 \leq i \leq m-2$, ab takes $(i, 0)$ to $(i+1, 0)$; hence all states in column 0 can be reached. State (i, j) can be reached from state $(i-j \pmod m, 0)$ by a^j . Therefore all the states are reachable.

It remains to prove that all the states are pairwise distinguishable. Let H (for *horizontal*) be the set $H = \{(m-1, 0), \dots, (m-1, n-2)\}$, and let V (for *vertical*) be $V = \{(0, n-1), \dots, (m-2, n-1)\}$. Given a state (i, j) , we define $d_{i,j}$ to be the minimal integer such that $a^{d_{i,j}}$ takes (i, j) to a final state, or infinity, if no final state is reachable by a 's from (i, j) . This depends on the boolean operation, and $d_{i,j} = 0$ if and only if (i, j) is final.

The boolean operations are now considered one by one.

Union: The final states are those in $H \cup V \cup \{(m-1, n-1)\}$. We may write $d_{i,j} = \min\{m-1-i, n-1-j\} \leq m-1$.

Let (i, j) and (k, l) be two distinct states, with $d_{i,j} \leq d_{k,l}$. If $d_{i,j} < d_{k,l}$, then the two states are distinguished by $a^{d_{i,j}}$. If $d_{i,j} = d_{k,l} = d$, apply a^{d+1} to both states. The resulting states must be distinct and each must have at least one zero component.

If the two states are of the form $(0, n-1-g)$ and $(0, n-1-h)$, $h < g$, then $(ab)^h$ distinguishes them. A symmetric argument works for $(m-1-g, 0)$ and $(m-1-h, 0)$. Suppose now the states are $(0, n-1-g)$ and $(m-1-h, 0)$. If $g \neq h$, then the states are distinguished by $(ab)^{\min\{g,h\}}$. If $g = h$, then applying $(ab)^{g+1}$ results in the two states $(1, 0)$ and $(0, 1)$. Since $d_{1,0} < d_{0,1}$ (because $m < n$), these two states are distinguished by $d_{1,0}$.

Symmetric Difference: The final states are those in $H \cup V$.

The removal of $(m-1, n-1)$ from the set of final states causes all of the $d_{i,j}$ to increase by m when $m-i = n-j$, and leaves the rest unchanged. Since all of the other $d_{i,j}$ are at most $m-1$, and the change maps distinct $d_{i,j}$ to distinct $d'_{i,j}$, the same argument for unequal $d_{i,j}$ applies to all pairs involving at least one of the states affected by the change. Since state $(m-1, n-1)$ was never used to distinguish equal $d_{i,j}$ cases in union, all remaining equality cases can be dealt with in the same way as in union.

Difference: The final states are those in H .

In this case only, we do not assume $m < n$. The $d_{i,j}$ here are as follows: $d_{i,j} = m-1-i$ if $m-i \neq n-j$, and otherwise $d_{i,j} = 2m-1-i$. The same distinguishability argument applies when $d_{i,j} \neq d_{k,l}$. Suppose $d_{i,j} = d_{k,l}$. Then $i = k$, and hence $j \neq l$. Apply a^{m-i} to get two distinct states $(0, g)$ and $(0, h)$, $g \neq 0$. As repeated applications of ab cycle through states $(0, 1), (0, 2), \dots, (0, n-1)$, there exists a d such that $(ab)^d$ sends $(0, g)$ to $(0, n-m)$, and $(0, h)$ to a different state. Therefore applying $(ab)^d a^{m-1}$ maps $(0, g)$ to a non-final state, and $(0, h)$ to a final state.

Intersection: The only final state is $(m-1, n-1)$.

We assume that $m < n$. If $\gcd(m, n) = 1$, then by the Chinese Remainder Theorem there is a bijection between the integers $\{0, 1, \dots, mn-1\}$ and the states of the direct product given by $k \leftrightarrow (k \pmod m, k \pmod n)$. Applying

a to the state corresponding to k results in the state corresponding to $k + 1$. Thus, for state (i, j) corresponding to k , $d_{i,j} = mn - 1 - k$; hence all states are distinguishable by multiple applications of a .

Now suppose $\gcd(m, n) > 1$. The states which can reach $(m - 1, n - 1)$ through multiple applications of a are exactly those which can be written in the form $(k \pmod{m}, k \pmod{n})$ for some integer k . Let S denote the set of these states. Any two states in S have different finite values of $d_{i,j}$, and hence are distinguishable.

Let $(i, j), (k, l) \notin S$; that is, $d_{i,j} = d_{k,l} = \infty$. These states can be distinguished from states in S using only a 's. Suppose $i \neq k$. Apply a^{m-i} to get two distinct states $(0, j')$ and (k', l') , $k' \neq 0$. Since $(0, j') \notin S$, $j' \neq 0$. As $m < n$ and $(0, m) \in S$, there exists a d such applying $(ab)^d$ to $(0, j')$ results in $(0, m)$. Then let d be the minimal integer such that applying $(ab)^d$ to the two states results in at least one state in S . Because the two resulting states are distinct, they must be distinguishable. \square

3 Boolean Operations with One Reversed Argument

Gao and Yu [8] studied the complexities of $K_m \cup L_n^R$ and $K_m \cap L_n^R$, and showed that they are both $m2^n - (m - 1)$, with quaternary witnesses. These results can be improved and extended as follows: (1) *ternary alphabets* suffice, (2) the *same language stream* can be used for K_m and L_n for both union and intersection, (3) the same language stream is also a witness for two *difference* operations and *symmetric difference*, and (4) the bound for symmetric difference is $m2^n$.

The reverse \mathcal{N}^R of an NFA \mathcal{N} is obtained by interchanging the sets of initial and final states and reversing all transitions.

Let $\mathcal{D}_1 = (Q_1, \Sigma, \delta_1, 0, \{m - 1\}) = \mathcal{U}_m(a, b, c)$ and $\mathcal{D}_2 = (Q_2, \Sigma, \delta_2, 0, \{n - 1\}) = \mathcal{U}_n(a, b, c)$, where $Q_1 = \{0, \dots, m - 1\}$ and $Q_2 = \{0, \dots, n - 1\}$. Let \mathcal{N}_2 be the NFA obtained by reversing \mathcal{D}_2 and let \mathcal{R}_2 be the DFA obtained from \mathcal{N}_2 by the subset construction. Since the reverse of \mathcal{N}_2 is deterministic, the subset construction applied to \mathcal{N}_2 results in a minimal DFA, by a theorem from [1]. Let \mathcal{P} be the direct product of \mathcal{D}_1 and \mathcal{R}_2 . The states of \mathcal{P} are of the form (i, S) , where $S \subseteq Q_2$. The problem is illustrated in Fig. 4, where DFA \mathcal{D}_1 has $m = 4$ and NFA $\mathcal{N}_2 = \mathcal{D}_2^R$ has $n = 5$.

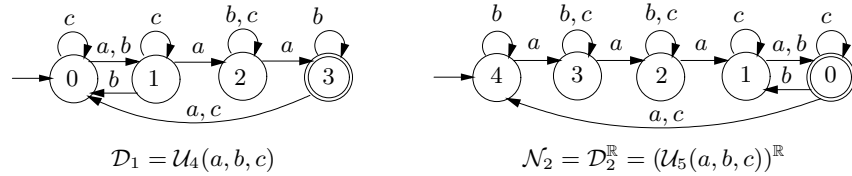


Fig. 4. DFA $\mathcal{D}_1 = \mathcal{U}_4(a, b, c)$ and NFA $\mathcal{N}_2 = \mathcal{D}_2^R = (\mathcal{U}_5(a, b, c))^R$.

First we derive upper bounds for two differences and for symmetric difference.

Proposition 1. *Let K_m and L_n be two regular languages with complexities m and n . Then the complexities of $K_m \setminus L_n^R$ and $L_n^R \setminus K_m$ are at most $m2^n - (m-1)$, and that of $K_m \oplus L_n^R$ is at most $m2^n$.*

Proof. Let $\mathcal{D}_1 = (Q_1, \Sigma, \delta_1, q_1, F_1)$ and $\mathcal{D}_2 = (Q_2, \Sigma, \delta_2, q_2, F_2)$ be the minimal DFA's of K_m and L_n . Consider the direct product \mathcal{P} of \mathcal{D}_1 and \mathcal{D}_2 , which is the determinized version of \mathcal{D}_2^R . With appropriate assignments of final states, \mathcal{P} can accept the languages $K_m \setminus L_n^R$, $L_n^R \setminus K_m$, and $K_m \oplus L_n^R$. The states of \mathcal{P} are of the form (i, S) where $i \in Q_1$ and $S \subseteq Q_2$. Therefore there are at most $m2^n$ states in \mathcal{P} , thus proving the bound for $K_m \oplus L_n^R$.

Note that any state of the form (i, \emptyset) is mapped to a state of the same form under any input $x \in \Sigma$. Also, any state of the form (i, Q_2) is mapped to a state of the same form since \mathcal{D}_2 is complete. For $K_m \setminus L_n^R$, all m states of the form (i, Q_2) are non-final, and thus indistinguishable. For $L_n^R \setminus K_m$, all m states of the form (i, \emptyset) are non-final and indistinguishable. Therefore \mathcal{P} contains at most $m2^n - (m-1)$ distinguishable states for $K_m \setminus L_n^R$ and $L_n^R \setminus K_m$. \square

Theorem 2 ($K \circ L^R$). *For $m, n \geq 3$, the complexities of the four languages $U_m(a, b, c) \cup (U_n(a, b, c))^R$, $U_m(a, b, c) \cap (U_n(a, b, c))^R$, $U_m(a, b, c) \setminus (U_n(a, b, c))^R$, and $(U_n(a, b, c))^R \setminus U_m(a, b, c)$ are all $m2^n - (m-1)$, and that of $U_m(a, b, c) \oplus (U_n(a, b, c))^R$ is $m2^n$.*

Proof. Let $K_m = \mathcal{U}_m(a, b, c)$ and $\mathcal{L}_n = \mathcal{U}_n(a, b, c)$; the various related automata are defined as above. It is known from [4] that the complexity of L_n^R is 2^n ; hence that of $K_m \circ L_n^R$ is at most $m2^n$. We first show that all $m2^n$ states of \mathcal{P} are reachable.

The initial state is $(0, \{n-1\})$. We have $(0, \{n-1\}) \xrightarrow{c} (0, \emptyset) \xrightarrow{a^i} (i, \emptyset)$ for $i = 1, \dots, n-1$. Input ab acts on \mathcal{N}_2 as the cycle $(n-1, n-2, \dots, 2, 0)$ and sends 0 to 0 in \mathcal{D}_1 . Therefore all states of the form $(0, \{j\})$ with $j \neq 1$ are reachable from $(0, \{n-1\})$ by repeated applications of ab . If $n \nmid m$, then $\{1+m \pmod{n}\} \neq \{1\}$ and $(0, \{1\})$ is reachable by a^m from $(0, \{1+m \pmod{n}\})$. If $n \mid m$, then $m-1 \equiv n-1 \pmod{n}$; so we have $(0, \{0\}) \xrightarrow{a^{m-1}} (m-1, \{1\}) \xrightarrow{c} (0, \{1\})$. For $i = 1, \dots, m-1$, $(i, \{j\})$ is reached from $(0, \{i+j \pmod{n}\})$ by a^i . So all states of the form (i, S) , where $|S| \leq 1$, are reachable.

Now suppose it is possible to reach all states of the form (i, S) , where $|S| = k$, $k \geq 1$. We want to show it is possible to reach all states (i, S) with $|S| = k+1$. The transformations a and b generate all permutations of states in \mathcal{N}_2 . Since $|S| \geq 2$, there is a word $w \in \{a, b\}^*$ and $S' \subseteq Q_2$ of size $k+1$ with $0, n-1 \in S'$ such that $S' \xrightarrow{w} S$. Moreover, w also causes a permutation of the states in \mathcal{D}_1 . Therefore it suffices to show the reachability of all states of the form (i, S) , where $|S| = k+1$ and $0, n-1 \in S$.

Let $S \subseteq Q_2$, $|S| = k+1$, and $0, n-1 \in S$. Define $S' = S \setminus \{n-1\}$. All states of the form (i, S') are reachable, and $(i, S') \xrightarrow{c} (i, S)$ for all $i \leq m-2$. For state $(m-1, S)$ there are three cases:

1. $m \nmid n$. State $m-1-n \pmod{m}$ is distinct from $m-1$. Therefore we have $(m-1-n, S) \xrightarrow{a^n} (m-1, S)$.
2. $m = n = 3$. Note that a^2ba is a transposition $(1, 2)$ in \mathcal{D}_1 and $(0, 2)$ in \mathcal{N}_2 . Thus $(1, S) \xrightarrow{a^2ba} (2, S)$, since $0, 2 \in S$.
3. $m \mid n$, $n \geq 4$. Define S'' to be the result of applying the transposition $a^2ba^{n-2} : (2, 3)$ in \mathcal{N}_2 to S' . So S'' is like S' with 2 and 3 transposed, if present. Since S' is S without $n-1$, and we have $0 \in S$, we also have $0 \in S'$ and $0 \in S''$. Applying c to S'' adds $n-1$. Applying ca^2ba^{n-2} to S'' adds $n-1$ and transposes 2 and 3, if present; hence the result is S . Since $m \mid n$, a^{n-2} is the same transformation as a^{m-2} in \mathcal{D}_1 ; hence a^2ba^{n-2} is the transposition $(m-2, m-1)$ in \mathcal{D}_1 . It follows that $(m-2, S'') \xrightarrow{ca^2ba^{n-2}} (m-1, S)$.

Therefore all $m2^n$ states are reachable, and it remains to find the number of pairwise indistinguishable states for each operation.

We claim that if $S, T \subseteq Q_2$ are distinct states of \mathcal{R}_2 , then there is an input which takes this pair of states to \emptyset and Q_2 . First suppose $0 \in S \setminus T$. Then applying c results in two states S_1 and T_1 such that $0, n-1 \in S_1 \setminus T_1$. For $k \geq 2$, define S_k and T_k as the states obtained by applying $a^{n-1}c$ to S_{k-1} and T_{k-1} , respectively. Then $0, 1, \dots, k-1, n-1 \in S_k \setminus T_k$. It follows that $S_{n-1} = Q_2$ and $T_{n-1} = \emptyset$. In general, if $j \in S \setminus T$, then applying a^j sends S and T to the case $0 \in S \setminus T$, and so the claim is true.

Sets Q_2 and \emptyset are mapped to themselves under all inputs $x \in \Sigma$. Also, Q_2 is final and \emptyset non-final in \mathcal{R}_2 . Therefore any states of the form (i, Q_2) and (j, \emptyset) are distinguishable for the boolean operations as follows:

- $K_m \cup L_n^R$, $L_n^R \setminus K_m$, and $K_m \oplus L_n^R$: apply a^k , $k \notin \{m-1-i, m-1-j\}$, to send i and j to non-final states.
- $K_m \cap L_n^R$: apply a^{m-1-i} so that i gets mapped to a final state.
- $K_m \setminus L_n^R$: apply a^{m-1-j} so that j gets mapped to a final state.

Thus any two states (i, S) and (j, T) with $S \neq T$ are distinguishable for all five boolean operations. Now consider states of the form (i, S) and (j, S) , $i < j$.

Case 1: $S = \emptyset$. Since all states of the form (i, \emptyset) are non-final for $K_m \cap L_n^R$ and $L_n^R \setminus K_m$, these states are indistinguishable. For the other three boolean operations, apply a^{m-1-j} to get the distinguishable states (k, \emptyset) , $(m-1, \emptyset)$, $k \neq m-1$.

Case 2: $S \neq \emptyset$, S is non-final (i.e., $0 \notin S$). In \mathcal{D}_1 , ba causes the cycle $(0, 2, 3, \dots, m-1)$, and in \mathcal{N}_2 , $ba : (n-1, n-2, \dots, 1)$. Since $i \neq j$, at least one of i and j is not equal to 1. Therefore we can apply $(ba)^d$ for some d so that the states become $(m-1, S')$, (k, S') where S' is non-final, and $k \neq m-1$. This distinguishes the states for $K_m \cup L_n^R$, $K_m \oplus L_n^R$, and $K_m \setminus L_n^R$. For the other two operations, apply a cyclic shift a^r so that S is mapped to some S'' and $0 \in S''$, and the pair of states is now in Case 3.

Case 3: $S \neq Q_n$, $0 \in S$. Again, apply $(ba)^p$ for some p so that the states become $(m-1, S')$, (k, S') , S' is final, and $k \neq m-1$. This distinguishes the

states for $K_m \cap L_n^R$ and $L_n^R \setminus K_m$. For the other three operations, apply a cyclic shift a^r so that S is mapped to S'' , and $0 \notin S''$, so that Case 2 now applies.

Case 4: $S = Q_n$. Since all states of the form (i, Q_2) are final for $K_m \cup L_n^R$ and non-final for $K_m \setminus L_n^R$, the states are indistinguishable for these cases. For the other three boolean operations, apply a^{m-1-j} to get the states (k, Q_2) , $(m-1, Q_2)$, $k \neq m-1$. This distinguishes the states.

Therefore for symmetric difference, all $m2^n$ states are distinguishable. For the other four operations, exactly m states are equivalent, thus proving the bounds in the theorem. \square

4 Boolean Operations with Two Reversed Arguments

Note that $(K \circ L)^R = K^R \circ L^R$ for all four boolean operations. Liu, Martin-Vide, A. Salomaa, and Yu [9] showed that $(2^m - 1)(2^n - 1) + 1$ is a tight upper bound for $K^R \cup L^R$ and $K^R \cap L^R$, and that the bound is met by ternary witnesses. We first derive upper bounds for difference and symmetric difference.

Proposition 2. *Let K_m and L_n be two regular languages with complexities m and n . Then the complexity of $K_m^R \setminus L_n^R$ is at most $(2^m - 1)(2^n - 1) + 1$, and the complexity of $K_m^R \oplus L_n^R$ is at most 2^{m+n-1} .*

Proof. Let $\mathcal{D}_1 = (Q_1, \Sigma, \delta_1, q_1, F_1)$ and $\mathcal{D}_2 = (Q_2, \Sigma, \delta_2, q_2, F_2)$ be the minimal DFA's of K_m and L_n . As in Proposition 1, we apply the standard subset construction to the NFA's \mathcal{N}_1 and \mathcal{N}_2 obtained by reversing \mathcal{D}_1 and \mathcal{D}_2 , and then construct their direct product DFA \mathcal{P} . The states of \mathcal{P} are of the form (S, T) where $S \subseteq Q_1$ and $T \subseteq Q_2$; hence \mathcal{P} has 2^{m+n} states.

For $K_m^R \setminus L_n^R$, all states of the form (\emptyset, T) and (S, Q_2) are non-final. Moreover, because \mathcal{D}_2 is complete, applying any input $x \in \Sigma$ leads to a state of the same form. Therefore these states are indistinguishable. As there are $(2^m - 1)(2^n - 1)$ states *not* of this form, \mathcal{P} has at most $(2^m - 1)(2^n - 1) + 1$ distinguishable states.

For $K_m^R \oplus L_n^R$, we note that (S, T) is final if and only if (\bar{S}, \bar{T}) is final, where $\bar{S} = Q_1 \setminus S$ and $\bar{T} = Q_2 \setminus T$. Let $S \subseteq Q_1$ be a subset of states of \mathcal{N}_1 ; apply $x \in \Sigma$ to get a state S' . Then $i \in S'$ if and only if $\delta_1(i, x) \in S$. It follows that S and \bar{S} are mapped to a pair S', \bar{S}' , i.e., complementary states are mapped to complementary states in \mathcal{N}_1 and \mathcal{N}_2 . Therefore complementary states are indistinguishable. Since every state has exactly one complement, \mathcal{P} has at most 2^{m+n-1} distinguishable states. \square

Next, we require a result concerning $\mathcal{U}_m(a, b, c)$ and $\mathcal{U}_n(b, a, c)$. The NFA's $\mathcal{N}_1 = (\mathcal{U}_4(a, b, c))^{\mathbb{R}}$ and $\mathcal{N}_2 = (\mathcal{U}_5(b, a, c))^{\mathbb{R}}$ are shown in Fig. 5, if the initial states are taken to be 3 and 4 as shown by the dotted arrows.

Lemma 1. *For $m, n \geq 3$, the complexities of $(\mathcal{U}_m(a, b, c))^R \cup (\mathcal{U}_n(b, a, c))^R$, $(\mathcal{U}_m(a, b, c))^R \cap (\mathcal{U}_n(b, a, c))^R$ and $(\mathcal{U}_m(a, b, c))^R \setminus (\mathcal{U}_n(b, a, c))^R$ are $(2^m - 1)(2^n - 1) + 1$, whereas that of $(\mathcal{U}_m(a, b, c))^R \oplus (\mathcal{U}_n(b, a, c))^R$ is 2^{m+n-1} , except when $m = n = 4$; then the first three complexities are 202 and the fourth is 116.*

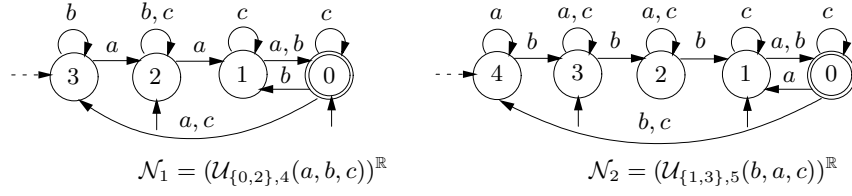


Fig. 5. NFA's $\mathcal{N}_1 = (\mathcal{U}_{\{0,2\},4}(a,b,c))^\mathbb{R}$ and $\mathcal{N}_2 = (\mathcal{U}_{\{1,3\},5}(b,a,c))^\mathbb{R}$.

Proof. Let $\mathcal{D}_1 = (Q_1, \Sigma, \delta_1, 0, \{m-1\})$ and $\mathcal{D}_2 = (Q_2, \Sigma, \delta_2, 0, \{n-1\})$ be the minimal DFA's of $\mathcal{U}_m(a,b,c)$ and $\mathcal{U}_m(b,a,c)$. Let \mathcal{N}_1 and \mathcal{N}_2 be the NFA's obtained by reversing \mathcal{D}_1 and \mathcal{D}_2 . Let \mathcal{R}_1 and \mathcal{R}_2 be the DFA's obtained from \mathcal{N}_1 and \mathcal{N}_2 by the subset construction. Since the reverses of \mathcal{N}_1 and \mathcal{N}_2 is deterministic, \mathcal{R}_1 and \mathcal{R}_2 are minimal [1]. Let \mathcal{P} be the direct product of \mathcal{R}_1 and \mathcal{R}_2 . The states of \mathcal{P} are of the form (S, T) where $S \subseteq Q_1$ and $T \subseteq Q_2$.

We first show that all 2^{m+n} states of \mathcal{P} are reachable if it is not the case that $m = n = 4$. The initial state is $(\{m-1\}, \{n-1\})$. From this state, (\emptyset, \emptyset) is reached by c . Also, $(\{m-1\}, \{n-1\}) \xrightarrow{bc} (\emptyset, \{n-2\}) \xrightarrow{b^{n-2-j}} (\emptyset, \{j\})$ for $j < n-2$, and $(\emptyset, \{0\}) \xrightarrow{b} (\emptyset, \{n-1\})$. Similarly, $(\{m-1\}, \{n-1\}) \xrightarrow{aca^{m-2-i}} (\{i\}, \emptyset)$ for $i \leq m-2$, and $(\{0\}, \emptyset) \xrightarrow{a} (\{m-1\}, \emptyset)$.

For $i, j \geq 2$, $(\{m-1\}, \{n-1\}) \xrightarrow{a^{m-1-i}b^{n-1-j}} (\{i\}, \{j\})$. For the other four states, we have the transformations $(\{2\}, \{3\}) \xrightarrow{ab^2} (\{1\}, \{1\}) \xrightarrow{a} (\{0\}, \{0\})$ and $(\{2\}, \{2\}) \xrightarrow{ab^2} (\{1\}, \{0\}) \xrightarrow{a} (\{0\}, \{1\})$. Therefore all states of the form (S, T) with $|S|, |T| \leq 1$ are reachable.

Suppose all states of the form $(\{i\}, T)$ are reachable for $|T| = k$, $k \geq 1$. Let $T \subseteq Q_2$ with $|T| = k+1$ and $0, n-1 \in T$. Let $T' = T \setminus \{n-1\}$. Then $(\{i\}, T') \xrightarrow{c} (\{i\}, T)$ for $1 \leq i \leq m-2$. Also, $(\{1\}, T) \xrightarrow{a^2} (\{m-1\}, T)$ and $(\{2\}, T) \xrightarrow{a^2} (\{0\}, T)$. Therefore all states of the form $(\{i\}, T)$ with $|T| = k+1$, $0, n-1 \in T$ are reachable. By the same argument as in Theorem 2, all states of the form $(\{i\}, T)$ with $|T| = k+1$ are reachable.

Now suppose all states of the form (S, T) are reachable for $|S| = k \geq 1$. Again, it suffices to consider only the subsets $S \subseteq Q_1$ of size $k+1$ with $0, m-1 \in S$, and show these (S, T) are reachable. Let $S' = S \setminus \{m-1\}$; then $S' \xrightarrow{c} S$. If 0 and $n-1$ are both in T or both not in T , then $T \xrightarrow{c} T$; hence $(S', T) \xrightarrow{c} (S, T)$. For the other T , we divide the problem into two cases.

Case 1: m is odd. Let $w \in \{a, b\}^*$ be a permutation of states on \mathcal{N}_1 and \mathcal{N}_2 . We show how to construct another word $w' \in \{a, b\}^*$ which performs the same transformation as w on \mathcal{N}_2 , but maps S to itself in \mathcal{N}_1 . To do this, we make three changes to w :

- (i) Add a^{m-1} to the beginning of w .
- (ii) Replace all instances of a in w by a^m .

(iii) Add a^{m+1} to the end of w .

Call the resulting word w' . Because m is odd and $a^2 : \mathbf{1}_{Q_2}$ on \mathcal{N}_2 , w' is the same transformation as w on \mathcal{N}_2 . Consider applying w' to S . Change (i) maps S to some S' with $0, 1 \in S'$. Since both a^m and b map S' to itself, the transformation caused by change (ii) maps S' to itself. Finally, change (iii) is the inverse of (i), mapping S' back to S .

For any state $T \subseteq Q_2$ of size $k+1$, there is a word $w \in \{a, b\}^*$ which permutes T to T' , for some T' of size $k+1$ and $0, n-1 \in T'$. Using the above construction, (S, T) is reachable from (S, T') by some permutation word. Therefore all 2^{m+n} states are reachable for odd m . Since the two NFA's are symmetric, the same argument applies for reachability of all states if n is odd.

Case 2: m and n are both even. Suppose first that $1 \in S$, and that T is of the form $T = \{0, t_1, \dots, t_l\}$, $0 < t_1 < \dots < t_l$. Let $j = n-1-t_l$, $T' = \{0, t_1+j, \dots, t_{l-1}+j, n-1\}$, and $w = (ab)^j$. Since ab is the cycle $(n-1, n-2, \dots, 1)$ of length $n-1$ in \mathcal{N}_2 , $T' \xrightarrow{w} T$.

Define the words $tr_i = a^i b a^{m-i}$ that act as the transpositions $(i, i+1)$ in \mathcal{N}_1 . They act in \mathcal{N}_2 as b if i is even, and aba if i is odd. Using the tr_i , we show how to construct $w' \in \{a, b\}^*$ from w so that $T' \xrightarrow{w'} T$ and $S \xrightarrow{w'} S$. We may assume that j is even, as if j is odd the same transformation can be caused by $w = (ba)^{j+n-1}$. Since $0, 1, m-1 \in S$, $w' = (tr_0 tr_{m-1})^{j/2}$ maps T' to T and S to itself, and is the desired transformation. It follows that all states of the form (S, T) , $0, 1, m-1 \in S$, $|S| = k+1$, $0 \in T$ are reachable. From states of this form, any T can be reached by applying cyclic shifts b^j , which map S to itself.

Now suppose $i \in S$, $1 < i < m-1$, and this i minimal. If i is even, let $w = tr_{i-1} (tr_{m-1})^{n-1}$. Then there exists S' of size $k+1$ containing $0, m-1$, and $i-1$ such that $S' \xrightarrow{w} S$. Moreover, w acts as $(aba)^n : \mathbf{1}_{Q_2}$ on \mathcal{N}_2 , so $(S', T) \xrightarrow{w} (S, T)$ for all $T \subseteq Q_2$. If i is odd, let $w = tr_{i-1} tr_{i-2} tr_{i-1} tr_{m-1}$, which acts as the transformation $(i-2, i)(0, m-1)$ on \mathcal{N}_1 and $(ba)^4$ in \mathcal{N}_2 . Since $n-1$ is odd, applying w^{n-1} is the same transformation on \mathcal{N}_1 , while becoming the identity on \mathcal{N}_2 (as ba causes a cycle of length $n-1$). Applying it to (S', T) for some S' containing $0, i-2, m-1$ results in (S, T) . It follows by induction on i that all states $S \cup T$ with $|S| = k+1$, and $\{0, m-1\} \subsetneq S$ are reachable.

Finally, suppose $S = \{0, m-1\}$. If $m \geq 6$, applying a^2 does not change \mathcal{N}_2 , but maps S to $S' = \{m-2, m-3\}$; thus $0, 1, m-1 \notin S'$. Reachability for all states of the form $S' \cup T$ follows from the same argument as the case $0, 1, m-1 \in S$. Since n is even, $(S', T) \xrightarrow{a^{n-2}} (S, T)$, and all of these states are reachable as well. By symmetry, this argument applies when $n \geq 6$.

The only case remaining is $m = n = 4$. Computation shows that only 232 of the possible 256 states are reachable.

Next we examine the distinguishability of the reachable states. Let (S_1, T_1) and (S_2, T_2) be two distinct states of \mathcal{P} , with $S_1 \neq S_2$. We may apply a cyclic shift b^k if necessary so that for each $i = 1, 2$, either (1) $T_i \in \{\emptyset, Q_2\}$, or (2) $\emptyset \subsetneq T_i \cap \{0, 1, \dots, n-2\} \subsetneq \{0, 1, \dots, n-2\}$. This is possible because $n \geq 3$.

Applying a cyclic shift a^l if necessary, we may assume that $0 \in S_1 \setminus S_2$. As in Theorem 2, we map S_1 to Q_1 and S_2 to \emptyset by applying $(ca^{m-1})^{m-2}$.

If the T_i are \emptyset or Q_2 , this transformation leaves them unchanged. Otherwise, by the above condition, they are not mapped to either \emptyset or Q_2 . Therefore we can map any pair of states of the form (S_1, T_1) and (S_2, T_2) , $S_1 \neq S_2$ to (Q_1, T'_1) , (\emptyset, T'_2) with $T'_i \in \{\emptyset, Q_2\} \iff T_i \in \{\emptyset, Q_2\}$ for $i = 1, 2$. A similar claim holds for the case $T_1 \neq T_2$ by switching the a 's and b 's.

We now consider each of the boolean operations separately.

Union: The states (Q_1, T) and (S, Q_2) are final for all possible S and T , and are all indistinguishable because any input leads to a state of the same form.

We now consider the $(2^m - 1)(2^n - 1)$ states not containing Q_1 or Q_2 , and show they are all distinguishable. By the above claim, and since the two DFA's are symmetric, we can reduce all pairs to the form (Q_1, T_1) , (\emptyset, T_2) , where $T_1, T_2 \neq Q_2$. These states are distinguishable by applying a cyclic shift b^k mapping T_2 to a non-final state.

Intersection: The states (\emptyset, T) and (S, \emptyset) are non-final and indistinguishable for all possible S and T . By the above claim again, all other states (not containing an \emptyset) can be reduced to the case (Q_1, T_1) , (\emptyset, T_2) , $T_1, T_2 \neq \emptyset$. Mapping T_1 to a final state using a cyclic shift will distinguish the states.

Difference: We consider the operation $U_m^R \setminus U_n^R$. The indistinguishable states are those of the form (\emptyset, T) and (S, Q_2) , which are all non-final. For (Q_1, T_1) , (\emptyset, T_2) are distinguished by shifting T_1 to a non-final state, and (S_1, Q_2) , (S_2, \emptyset) are distinguished by shifting S_2 to a final state.

Symmetric difference We first note that (S, T) is final if and only if (\bar{S}, \bar{T}) is final. Moreover, one can verify that if two states are complementary, then they are mapped to complementary states under any input. Therefore (S, T) and (\bar{S}, \bar{T}) are indistinguishable. This leads to a maximum of 2^{n+m-1} distinguishable states.

For any state (S, T) , either S or \bar{S} contains q_0 . Therefore to complete the proof, we only need to show that all states of the form (S, T) with $q_0 \in S$ are distinguishable. Let (S_1, T_1) and (S_2, T_2) be two such states. If $T_1 = T_2$, then $S_1 \neq S_2$, there exists q_k such that $k \in S_1 \oplus S_2$, and hence a^k distinguishes the states. If $T_1 \neq T_2$, by applying b^2 if necessary, we may assume that there exists $k \in \{0, \dots, n-2\}$ such that $k \in T_1 \oplus T_2$. By applying ca^{m-1} , we may assume that $q_0, q_1 \in S_1 \cap S_2$. This does not change the fact that T_1 and T_2 are distinct, by the above assumption. So then applying b^k for $k \in T_1 \oplus T_2$ distinguishes the two states. \square

For $m \geq 3$, let $\mathcal{U}_{\{0,2\},m}(a,b,c)$ be the DFA obtained from $\mathcal{U}_m(a,b,c)$ by changing the set of final states to $\{0,2\}$. For $n \geq 4$, let $\mathcal{U}_{\{1,3\},n}(b,a,c)$ ($\{1,3\}$) be the DFA obtained from $\mathcal{U}_n(b,a,c)$ by changing the set of final states to $\{1,3\}$, and for $n = 3$, use $\mathcal{U}_{\{1\},n}(b,a,c)$ with final state 3.

Theorem 3 ($K^R \circ L^R$). *Let $K_m = \mathcal{U}_{\{0,2\},m}(a,b,c)$ and $L_n = \mathcal{U}_{\{1,3\},n}(b,a,c)$ for $n \geq 4$ and let $L_3 = \mathcal{U}_{\{1\},3}$. For $m, n \geq 3$, the complexities of $K_m^R \cup L_n^R$,*

$K_m^R \cap L_n^R$, and $K_m^R \setminus L_n^R$ are $(2^m - 1)(2^n - 1) + 1$, whereas that of $K_m^R \oplus L_n^R$ is 2^{m+n-1} .

Proof. If it is not the case $m = n = 4$, then by Lemma 1, it suffices to show that state $(\{m-1\}, \{n-1\})$ is reachable from the initial state of the NFA. If $n = 3$, the initial state is $(\{0, 2\}, \{1\})$. We have the chain $(\{0, 2\}, \{1\}) \xrightarrow{ab^2c} (\{1\}, \{1\}) \xrightarrow{a^2b^2} (\{m-1\}, \{n-1\})$.

Suppose $n \geq 4$. The initial state is $(\{0, 2\}, \{1, 3\})$. Apply the following: $(\{0, 2\}, \{1, 3\}) \xrightarrow{ac} (\{1\}, \{0, 3, n-1\}) \xrightarrow{a^3} (\{m-2\}, \{1, 3, n-1\})$. If $n = 4$, then $n-1 = 3$, and we can apply $(\{m-2\}, \{1, 3\}) \xrightarrow{c} (\{m-2\}, \{1\}) \xrightarrow{b^2a^{m-1}} (\{m-1\}, \{n-1\})$. If $n > 4$, then apply $(\{m-2\}, \{1, 3, n-1\}) \xrightarrow{cb^2c} (\{m-2\}, \{1\}) \xrightarrow{b^2a^{m-1}} (\{m-1\}, \{n-1\})$.

For every case except $m = n = 4$, this shows that all states are reachable. When $m = n = 4$, one can verify through explicit enumeration that the states unreachable from $(\{3\}, \{3\})$ are exactly the states reached from $(\{0, 2\}, \{1, 3\})$ by words in $\{a, b\}^*$. Therefore in this case all states are reachable as well. \square

5 Product and Star

5.1 The Language KL^R

Cui, Gao, Kari and Yu showed in [6] that the complexity of KL^R is $(m-1)2^n + 2^{n-1} - (m-1)$, with ternary witnesses. We now prove that the bound can also be met by one stream. The NFA \mathcal{N} for $U_4(a, b, c)(U_5(a, b, c))^R$ is shown in Fig. 6.

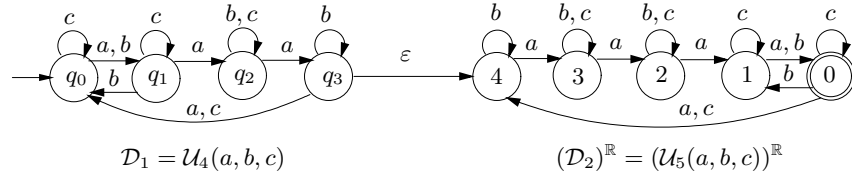


Fig. 6. NFA \mathcal{N} for $U_4(a, b, c)(U_5(a, b, c))^R$.

Theorem 4. For $m, n \geq 3$, the complexity of the product $U_m(a, b, c)(U_n(a, b, c))^R$ is $(m-1)2^n + 2^{n-1} - (m-1)$.

Proof. Let $\mathcal{D}_1 = (Q_1, \Sigma, \delta_1, q_0, \{q_{m-1}\})$ and $\mathcal{D}_2 = (Q_2, \Sigma, \delta_2, 0, \{n-1\})$ be the minimal DFA's of $U_m(a, b, c)$ and $U_n(a, b, c)$, where $Q_1 = \{q_0, \dots, q_{m-1}\}$ and

$Q_2 = \{0, \dots, n-1\}$. Let \mathcal{N}_2 be $\mathcal{D}_2^{\mathbb{R}}$, and let \mathcal{N} be the NFA for the product of \mathcal{D}_1 and \mathcal{N}_2 , as illustrated in Fig. 6.

We use the subset construction on \mathcal{N} to get a DFA \mathcal{P} for this product. Any state of \mathcal{P} must either not contain q_{m-1} , or contain both q_{m-1} and $n-1$. There are $(m-1)2^n$ states of the former type, and 2^{n-1} states of the latter. We will show that all of these states are reachable.

Set $\{q_0\}$ is initial, $\{q_i\}$ is reached by a^i , for $i = 1, \dots, m-2$, and $\{q_{m-1}, n-1\}$ by a^{m-1} . Also, $\{q_{m-1}, n-1\} \xrightarrow{a} \{q_0, n-2\}$, and from there $\{q_0, j\}$ is reached by $(ab)^{n-2-j}$ for $j = 2, \dots, n-3$, $\{q_0, 0\}$ by $(ab)^{n-3}$, and $\{q_0, n-1\}$ by $(ab)^{n-2}$.

If $n \nmid m$, then $\{1+m \pmod{n}\} \neq \{1\}$ and $\{q_0, 1\}$ is reachable by a^m from $\{q_0, 1+m \pmod{n}\}$. If $n \mid m$, then $m-1 \equiv n-1 \pmod{n}$; so applying $a^{m-1}c$ sends $\{q_0, 0\}$ to $\{q_0, 1\}$. For $i = 1, \dots, m-2$, $\{q_i, j\}$ is reached from $\{q_0, i+j \pmod{n}\}$ by a^i . So all states $\{q_i\} \cup S$, where $i < m-1$ and $|S| \leq 1$ are reachable.

For the rest of the proof S and T will denote subsets of Q_2 . Suppose it is possible to reach all states of the form $\{q_i\} \cup S$, where $i < m-1$, $S \subseteq Q_2$, and $|S| = k \geq 1$. We want to show it is possible to reach all states of the form $\{q_{m-1}\} \cup T$, $|T| = k+1$, and $n-1 \in T$. Let $T = \{t_1, \dots, t_k, n-1\}$. Then $\{q_{m-2}, (t_1+1), \dots, (t_k+1)\} \xrightarrow{a} \{q_{m-1}\} \cup T$, and this state is reachable.

Now suppose all states of the form $\{q_{m-1}\} \cup T$, where $|T| = k \geq 2$ and $n-1 \in T$ are reachable. We want to show that all states of the form $\{q_i\} \cup S$ with $|S| = k$ are reachable. Applying a shows that all states of the form $\{q_0\} \cup T$ with $|T| = k$ and $n-2 \in T$ are reachable. The word ab sends q_0 to q_0 , and acts as the cycle $(n-1, n-2, \dots, 2, 0)$ on the states of \mathcal{N}_2 . Hence for any subset $T' \subseteq Q_2$ of size $k \geq 2$, there exists an integer d and $T \subseteq Q_2$ containing $n-2$ such that $T \xrightarrow{(ab)^d} T'$. Therefore all states of the form $\{q_0\} \cup S$ with $|S| = k$ are reachable. Let $i < m-1$ and $S = \{s_1, \dots, s_k\} \subseteq Q_2$. State $\{q_i\} \cup S$ is reachable by a^i from state $\{q_0\} \cup \{s_1+i, \dots, s_k+i\}$, where addition is modulo n . Hence all states of the form $\{q_i\} \cup S$ with $i < m-1$ and $|S| = k+1$ are reachable.

Combining these two results shows that all the required states are reachable.

For distinguishability, first note that all m states of the form $\{q_i\} \cup Q_2$ are final and indistinguishable.

Suppose we have two states $\{q_i\} \cup S$ and $\{q_j\} \cup T$ with $S \neq T$. Let $k \in S \oplus T$; then a^k distinguishes the two states. Now consider the pair $\{q_i\} \cup S$, $\{q_j\} \cup S$, $S \neq Q_2$. Let $k \notin S$, and apply a^k to get $\{q_{i'}\} \cup S'$, $\{q_{j'}\} \cup T'$. If $S' \neq T'$, then by the previous argument the states are distinguishable. Otherwise, $S' = T'$ and $0 \notin S'$. So without loss of generality we may assume that $0 \notin S$. We know that ba acts as the cycle $(q_0, q_2, q_3, \dots, q_{m-1})$ on \mathcal{D}_1 , and maps only 0 to 0 in \mathcal{N}_2 . Since $i \neq j$, at least one of i, j is not equal to 1. Then by applying some $(ba)^d$ if necessary, we may assume that $i < m-2$, $j = m-2$. Apply a to get $\{q_{i+1}\} \cup T$, $\{q_{m-1}\} \cup T \cup \{n-1\}$, where $n-1 \notin T$. Since these states contain different subsets of Q_2 , they are distinguishable by the previous argument. \square

5.2 The Language $K^R L$

Let $\mathcal{V}_n(a, b, c, d) = (Q_{\mathcal{V}}, \Sigma, \delta_{\mathcal{V}}, 0, \{n-1\})$, where $Q = \{0, \dots, n-1\}$, $a : (0, \dots, n-1)$, $b : (n-2, n-1)$, $c : \binom{n-1}{n-2}$, and $d : \mathbf{1}_{Q_n}$. Let $V_n(a, b, c, d)$ be the language of $\mathcal{V}_n(a, b, c, d)$.

It was shown in [5] by Cui, Gao, Kari and Yu that $3 \cdot 2^{m+n-2}$ is a tight bound for $K_m^R L_n$. They used $\mathcal{V}_n(a, b, c, d)$ as witnesses K_m (some relabelling is needed), and L_n with $a, c : \mathbf{1}_{Q_n}$, $b : \binom{Q_n}{0}$, $d : (0, \dots, n-1)$ and final state $n-1$. We prove that the permutationally equivalent dialects $(V_m(a, b, c, d) \mid m \geq 3)$ and $(V_n(d, c, b, a) \mid n \geq 3)$ can also be used.

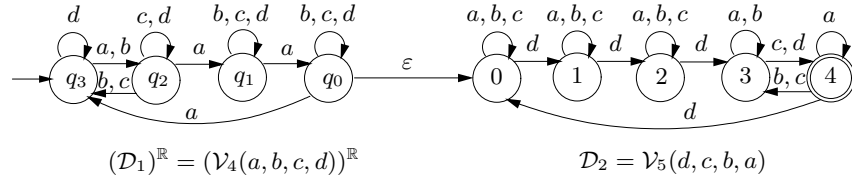


Fig. 7. NFA for $(V_4(a, b, c, d))^R V_5(d, c, b, a)$.

Theorem 5 ($K_m^R L_n$).

For $m, n \geq 3$, the complexity of $(V_m(a, b, c, d))^R V_n(d, c, b, a)$ is $3 \cdot 2^{m+n-2}$.

Proof. Let $\mathcal{D}_1 = (Q_1, \Sigma, \delta_1, q_0, \{q_{m-1}\})$ and $\mathcal{D}_2 = (Q_2, \Sigma, \delta_2, 0, \{n-1\})$ be the minimal DFA's of $V_m(a, b, c, d)$ and $V_n(d, c, b, a)$, where $Q_1 = \{q_0, \dots, q_{m-1}\}$ and $Q_2 = \{0, \dots, n-1\}$. Let \mathcal{N}_1 be \mathcal{D}_1^R , and let \mathcal{N} be the NFA for the product of \mathcal{N}_1 and \mathcal{D}_2 , as illustrated in Fig. 7.

We use the subset construction to get a DFA \mathcal{P} for this product. We claim that all 2^{m+n-1} states of \mathcal{P} not containing q_0 and all 2^{m+n-2} states containing q_0 and 0 are reachable.

The initial state is $\{q_{m-1}\}$. Then we have $\{q_{m-1}\} \xrightarrow{a^{m-1-i}} \{q_i\}$ for $i \geq 1$, and $\{q_{m-1}\} \xrightarrow{a^{m-1}} \{q_0, 0\}$. Now suppose all states of the form $S \subsetneq Q_1$, $|S| = k \geq 1$ are reachable. Let $S = \{q_{s_1}, \dots, q_{s_{k+1}}\}$ with $0 < s_1 < \dots < s_{k+1}$. Let $i = s_{k+1} - s_k - 1$, and $j = m - 1 - s_{k+1}$. Let $S' = \{q_{s_1+i+j}, \dots, q_{s_{k-1}+i+j}, q_{m-2}\}$. Note that S' is reachable. Then S is reachable by the sequence

$$S' \xrightarrow{c} S' \cup \{q_{m-1}\} \xrightarrow{(ab)^i} \{q_{s_1+j}, \dots, q_{s_{k-1}+j}, q_{s_k+j}, q_{m-1}\} \xrightarrow{a^j} S.$$

On the other hand, setting $s_1 = 0$ shows the reachability for all states of the form $S \cup \{0\}$, $|S| = k + 1$, $q_0 \in S$.

Suppose states of the form $S \cup T$ with $\emptyset \subsetneq S \subseteq Q_1 \setminus \{q_0\}$, $T \subseteq Q_2$, and $|T| = k \geq 0$ are reachable. Since S is non-empty, $S \xrightarrow{a^m} S \cup \{0\}$. Let $T =$

$\{t_1, \dots, t_{k+1}\}$, $t_1 < \dots < t_{k+1}$. Let $T' = \{t_2 - t_1, \dots, t_{k+1} - t_1\}$. By induction, $S \cup T'$ is reachable. Then $S \cup T$ is reachable by the sequence

$$S \cup T' \xrightarrow{a^m} S \cup \{0\} \cup T' \xrightarrow{d^{t_1}} S \cup T.$$

Moreover, if we take $S = \{q_{m-1}\}$, then $S \cup T \xrightarrow{c^2} T$.

Finally, consider states of the form $S \cup T$ where $q_0 \in S$, $0 \in T$. If $S \neq Q_1$, there exists an S' with $q_0 \notin S'$ such that $S' \cup T \xrightarrow{a^j} S \cup T$ for some j . Note that $S' \cup T$ is reachable by the previous case. If $S = Q_1$, then define $S' = Q_1 \setminus \{q_0\}$. Once again, $S' \cup T$ is reachable, and we have $S' \cup T \xrightarrow{ac^2} S \cup T$. Therefore all of the desired states are reachable.

We now prove that all of these states are distinguishable. Let $S_1 \cup T_1, S_2 \cup T_2$ be a pair of states, $S_1, S_2 \subseteq Q_1$, $T_1, T_2 \subseteq Q_2$. If $T_1 \neq T_2$, then let $k \in T_1 \oplus T_2$. The states are distinguishable by d^{n-1-k} . If $S_1 \neq S_2$ without loss of generality (applying a cyclic shift if necessary), assume $q_0 \in S_1 \oplus S_2$. Applying b^2 ensures that $n-1 \notin T_1 \cup T_2$. Then applying d transforms the pair to $S_1 \cup T'_1, S_2 \cup T'_2$, and $0 \in T'_i$ if and only if $q_0 \in S_i$. So $T'_1 \neq T'_2$, and the states are distinguishable. \square

5.3 The Language $(KL)^R = L^R K^R$

Let $\mathcal{U}_n(a, b, c, d) = (Q, \Sigma, \delta_{\mathcal{U}}, 0, \{n-1\})$, where $a : (0, \dots, n-1)$, $b : (0, 1)$, $c : \binom{n-1}{0}$, and $d : \mathbf{1}_Q$; thus $\mathcal{U}_n(a, b, c) = \mathcal{U}_n(a, b, c, \emptyset)$. Let $U_n(a, b, c, d)$ be the language of $\mathcal{U}_n(a, b, c, d)$.

It was shown by Cui, Gao, Kari, and Yu [5] that quaternary witnesses meet the bound $3 \cdot 2^{m+n-2} - 2^n + 1$ for $(K_m L_n)^R$. They used witness K_m with inputs (after relabelling) $a, b, c : \mathbf{1}_Q$, $d : (0, \dots, m-1)$, and final state $m-1$, and witness L_n with $a : (0, \dots, n-1)$, $b : (n-2, n-1)$, $c : \binom{n-1}{n-2}$, $d : \mathbf{1}_{Q_n}$ and final state $n-1$. Here L_n is a dialect of $U_n(a, b, c, d)$. We show that the languages $U_m(a, b, c, d)$ and $U_n(d, c, b, a)$ also work.

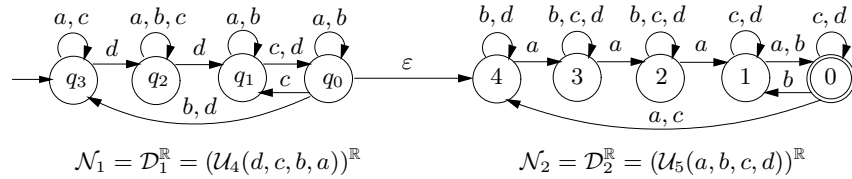


Fig. 8. NFA for $(U_4(d, c, b, a))^R (U_5(a, b, c, d))^R$.

Theorem 6 ($L_n^R K_m^R$). *The complexity of $(U_n(d, c, b, a))^R (U_m(a, b, c, d))^R$ is $3 \cdot 2^{m+n-2} - 2^n + 1$, for $m, n \geq 3$.*

Proof. Let $\mathcal{D}_1 = (Q_1, \Sigma, \delta_1, q_0, \{q_{n-1}\})$, where $Q_1 = \{q_0, \dots, q_{n-1}\}$, and $\mathcal{D}_2 = (Q_2, \Sigma, \delta_2, 0, \{m-1\})$, where $Q_2 = \{0, \dots, m-1\}$, be the minimal DFA's of $U_n(d, c, b, a)$ and $U_m(a, b, c, d)$. Let $\mathcal{N}_1 = \mathcal{D}_1^{\mathbb{R}}$, $\mathcal{N}_2 = \mathcal{D}_2^{\mathbb{R}}$, and let \mathcal{N} be the NFA for the product of \mathcal{N}_1 and \mathcal{N}_2 , as illustrated in Fig. 8. We use the subset construction to get a DFA \mathcal{P} for this product. Any reachable state of \mathcal{P} must either not contain q_0 or contain both q_0 and $n-1$. We will show that all 2^{n+m-1} and 2^{n+m-2} states of these two forms are reachable.

The initial state of \mathcal{P} is $\{q_{n-1}\}$. It is known from [4,10] that all 2^n subsets of Q_1 are reachable in \mathcal{N}_1 by words in $\{b, c, d\}^*$. Of these inputs, b and d map state $\{m-1\}$ of \mathcal{N}_2 to itself, and c maps $\{m-1\}$ to \emptyset . Suppose state $S \subseteq Q_1$ is reached by applying the word $w \in \{b, c, d\}^*$ to \mathcal{N}_1 . If $q_0 \in S$, then the state $S \cup \{q_{m-1}\}$ is reachable in \mathcal{P} by w . If $q_0 \notin S$, since c^2 is the identity transformation on \mathcal{N}_1 , state S of \mathcal{P} is reachable by $w c^2$.

We have the chain $\{q_{n-1}\} \xrightarrow{d^n} \{q_{n-1}, m-1\} \xrightarrow{b} \{m-1\}$. In a way similar to that in \mathcal{N}_1 , all 2^m subsets of Q_2 are reachable in \mathcal{N}_2 by words in $\{a, b, c\}^*$. Applying the same words to $\{m-1\}$ in \mathcal{P} yields all subsets of Q_2 .

Now suppose that all states of the form $S \cup T$, $S \subseteq Q_1 \setminus \{q_0\}$, $T \subseteq Q_2$, $|T| = k \geq 0$ are reachable. We will show that all states of the form $S \cup T$, $|T| = k+1$ are reachable. Let $T = \{t_1, t_2, \dots, t_{k+1}\}$, $t_1 < \dots < t_{k+1}$. Let $S \subseteq Q_1 \setminus \{q_0\}$. We have already established that if $S = \emptyset$, $S \cup T$ is reachable. Otherwise, define $j = m-1 - t_{k+1}$, and $T' = \{t_1 + j, t_2 + j, \dots, t_k + j\}$. Then $S \cup T' \xrightarrow{d^n} S \cup T' \cup \{m-1\} \xrightarrow{a^j} S \cup T$.

Now suppose $q_0 \in S$. If $S \neq Q_1$, there exists an S' with $q_0 \notin S'$ such that $S' \cup T \xrightarrow{a^j} S \cup T$ for some j . Note that $S' \cup T$ is reachable by the previous case. If $S = Q_1$, then define $S' = Q_1 \setminus \{q_0\}$. Once again, $S' \cup T$ is reachable, and we have $S' \cup T \xrightarrow{d b^2} S \cup T$.

Therefore all $2^{n+m-1} + 2^{n+m-2} = 3 \cdot 2^{n+m-2}$ states not containing q_0 or containing both q_0 and $m-1$ are reachable.

For distinguishability, first note that all 2^n states of the form $S \cup Q_2$ are final and indistinguishable. Consider a pair of states $S_1 \cup T_1, S_2 \cup T_2$, with $S_1, S_2 \subseteq Q_1$ and $T_1, T_2 \subsetneq Q_2$. If $T_1 \neq T_2$, let $k \in T_1 \oplus T_2$; then a^k distinguishes the states. Otherwise, $T_1 = T_2 = T$, and $S_1 \neq S_2$. Since $T \neq Q_2$, there exists a $k \notin T$. Also, there exists $q_l \in S_1 \oplus S_2$. Applying $d^l a^{k+1}$ results in states $S'_1 \cup T'_1, S'_2 \cup T'_2$ such that $m-1 \in T'_1 \oplus T'_2$. Therefore all remaining states are distinguishable by using the previous argument. \square

5.4 Reverse of Star

Note that $(L^*)^R = (L^R)^*$. The star of the reverse was studied by Gao, K. Salomaa, and Yu [7], who showed that the complexity of this operation is 2^n . The witness they used is a dialect of $U_n(a, b, c)$. After relabelling of states and permuting the inputs, it has the following transformations: $a : (0, \dots, n-1)$, $b : (0, n-1)$ and $c : \binom{0}{n-1}$, and the final state is 0. The witness $\mathcal{U}_{\{0\},n}(a, b, c)$, which is $\mathcal{U}_n(a, b, c)$ with final state set changed to $\{0\}$ also works, as does every dialect of $\mathcal{U}_n(a, b, c)$ with final state set $\{0\}$.

Theorem 7 $((L^*)^R)$. For $n \geq 3$, the complexity of $((U_{\{0\},n}(a, b, c))^*)^R$ is 2^n .

Proof. The proof is the same as that in [7]. Since L_n has only one final state which is also the initial state, we have $L_n^* = L_n$. Hence $(L_n^*)^R = L_n^R$, and L_n^R has state complexity 2^n . \square

6 Conclusions

We have proved that the universal witnesses $U_n(a, b, c)$ and $U_n(a, b, c, d)$, along with their permutational equivalents $U_n(b, a, c)$ and $U_n(d, c, b, a)$, and dialects $U_{\{0,2\},m}(a, b, c)$, $U_{\{1,3\},n}(a, b, c)$, $U_{\{0\},n}(a, b, c)$, $V_m(a, b, c, d)$ and $V_n(d, c, b, a)$ suffice to act as witnesses for all the state complexity bounds involving binary boolean operations, product, star and reversal. We have shown that it is efficient to consider all four boolean operations together. Lastly, the use of universal witnesses and their dialects simplified many proofs, and allowed us to utilize the similarities in the witnesses.

Acknowledgment We thank Baiyu Li for careful proofreading.

References

1. Brzozowski, J.: Canonical regular expressions and minimal state graphs for definite events. In: Proceedings of the Symposium on Mathematical Theory of Automata. Volume 12 of MRI Symposia Series, Polytechnic Press, Polytechnic Institute of Brooklyn, N.Y. (1963) 529–561
2. Brzozowski, J.: Quotient complexity of regular languages. *J. Autom. Lang. Comb.* **15**(1/2) (2010) 71–89
3. Brzozowski, J.: In search of the most complex regular languages. In Moreira, N., Reis, R., eds.: Proceedings of the 17th International Conference on Implementation and Application of Automata (CIAA). Volume 7381 of LNCS, Springer (2012) 5–24
4. Brzozowski, J., Tamm, H.: Quotient complexity of atoms of regular languages. In Yen, H.C., Ibarra, O.H., eds.: Proceedings of the 16th International Conference on Developments in Language Theory (DLT). Volume 7410 of Lecture Notes in Computer Science, Springer (2012) 50–61
5. Cui, B., Gao, Y., Kari, L., Yu, S.: State complexity of combined operations with two basic operations. *Theoret. Comput. Sci.* **437** (2012) 82–102
6. Cui, B., Gao, Y., Kari, L., Yu, S.: State complexity of two combined operations: catenation-star and catenation-reversal. *Int. J. Found. Comput. Sc.* **23**(1) (2012) 51–66
7. Gao, Y., Salomaa, K., Yu, S.: The state complexity of two combined operations: star of catenation and star of reversal. *Fund. Inform.* **83**(1–2) (2008) 75–89
8. Gao, Y., Yu, S.: State complexity of combined operations with union, intersection, star, and reversal. *Fund. Inform.* **116** (2012) 1–14
9. Liu, G., Martin-Vide, C., Salomaa, A., Yu, S.: State complexity of basic language operations combined with reversal. *Inform. and Comput.* **206** (2008) 1178–1186
10. Salomaa, A., Wood, D., Yu, S.: On the state complexity of reversals of regular languages. *Theoret. Comput. Sci.* **320** (2004) 315–329
11. Yu, S.: State complexity of regular languages. *J. Autom. Lang. Comb.* **6** (2001) 221–234